The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud

By Richard J. Sullivan

The fraudsters, phishers, hackers, and pickpockets who thrive off payment card fraud may soon have their work cut out for them. U.S. financial institutions have announced plans to add computer chips to their debit and credit cards in the next few years, a move likely to make payment card fraud more difficult. Compared with the magnetic-stripe payment cards carried by millions of U.S. consumers, the new chip cards will offer stronger defenses against fraud. But they certainly will not put an end to it.

In fact, as countries around the world have adopted computer-chip cards, new trends in fraud have emerged. France, the Netherlands, and the United Kingdom all switched from magnetic-stripe to computer-chip payment cards, with mixed results. The fraudulent use of lost and stolen cards declined in both France and the United Kingdom. But fraudsters soon shifted tactics and exploited other weak links in payment card security. In the United Kingdom, the eventual success at responding effectively to new trends in fraud depended, in part, on a system of fraud data collection and monitoring that is lacking in the United States.

Richard J. Sullivan is a senior economist at the Federal Reserve Bank of Kansas City. This article is on the bank's website at ***www.KansasCityFed.org.***

This article examines how computer-chip cards work differently from magnetic-stripe cards, describes the security improvements offered by the chips, and reviews their mixed track record at defeating fraud in other countries. Evidence from overseas suggests any prolonged accommodation of older-card technology during a transition to computer-chip cards can allow fraudsters to exploit weak links in card security. Reliance on low-cost authentication methods also invites growth in fraud. U.S. regulators and industry leaders should expect shifts in the nature of payment card fraud and take proactive countermeasures. But the United States currently lacks effective tools to gauge what types of fraud are on the rise. Establishing a comprehensive monitoring system could help in assessing the level of payment card fraud, tracking trends in the fraud, and measuring the losses sustained by its victims.

Section I reviews the distinct types payment card fraud and the security weaknesses in magnetic-stripe payment cards. Section II describes how computer chips can improve security and reviews how adoption of the new cards affected fraud patterns in France, the Netherlands, and the United Kingdom. Section III considers the implications for the United States of other countries' experiences with computer-chip card adoption.

I. PAYMENT CARD FRAUD AND MAGNETIC-STRIPE CARDS

Only a small proportion of payment card transactions are fraudulent, but the losses are large because the total volume of payment card use in the United States is immense. U.S. cardholders used more than one billion debit and credit cards in 2011, making 69 billion transactions, valued at more than $3.9 trillion (Nilson Report 2012a, 2012b; Federal Reserve Board). These payment card transactions accounted for roughly 60 percent of all noncash retail payments in the country. Even a small fraction of that kind of volume can amount to billions of dollars in losses for banks and merchants. In 2009, payment card fraud losses in the United States totaled an estimated $3.4 billion (Table 1).[1]

Fraud trends and prevention methods

Payment card issuers report that three forms of compromised security account for most fraudulent transactions: lost or stolen cards, card

Table 1
LOSSES DUE TO FRAUD ON CARD PAYMENTS
United States, 2009

	Loss per Dollar	Value of Transactions in millions	Value of Loss[2] in millions
PIN Debit Cards	0.0319%	$563,100	$179.6
Signature Debit Cards	0.1271%	$857,500	$1,089.9
General Purpose Credit Cards	0.1271%[1]	$1,714,000	$2,178.5
Prepaid Cards	0.0401%	$140	$0.6
Total		$3,134,740	$3,448.1

Note: The estimates in this table are for losses on purchase transactions for both merchants and card issuers.
[1]The loss rate for general-purpose credit cards is assumed to be the same as the loss rate for signature debit cards. General-purpose credit cards and signature debit cards use similar authentication and approval protocols.
[2]Value of loss is the product of loss per dollar and value of transactions.
Sources: Figures for loss per dollar are from Board of Governors. Figures for value of transactions are from Federal Reserve System.

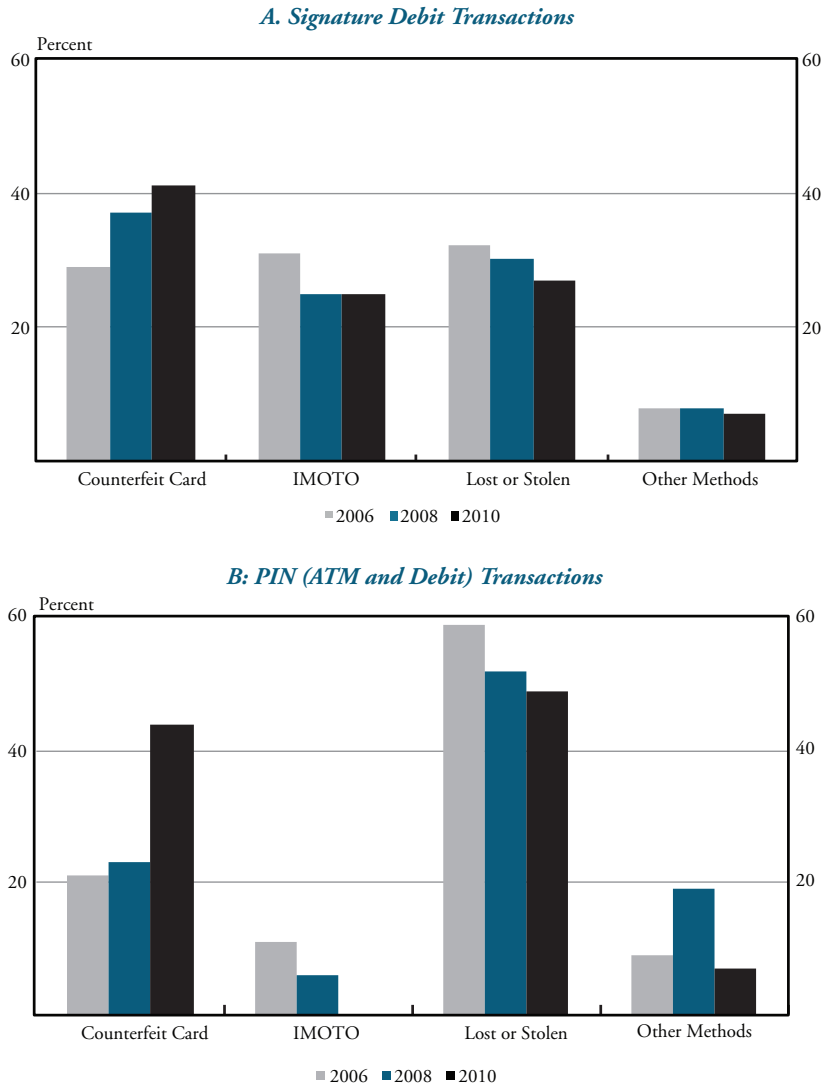
counterfeiting, and fraudulent purchases made by Internet, mail order, and telephone order (IMOTO).[2] Fraud types and rates of success differ for card payments authorized by signature and those authorized by personal identification number (PIN).[3] Because forging signatures is easier than stealing PINs, the loss per dollar for signature-authorized payments is significantly higher than losses for PIN payments (Table 1).[4]

For signature debit cards, the most common category of security compromise in 2006 was lost or stolen cards, accounting for 32 percent of all signature debit fraud that year. By 2010, however, lost or stolen cards as a share of all signature debit fraud had fallen to 27 percent (Chart 1, Panel A). Fraud on IMOTO transactions also declined from 31 percent to 25 percent as a share of total signature debit over the 2006-2010 period, while card counterfeiting rose from 29 percent to 41 percent and became the foremost category of signature debit fraud.

For PIN-authorized transactions (whether by debit purchase or ATM withdrawal), the primary categories of compromise have been lost or stolen cards and card counterfeiting (Chart 1, Panel B). In 2006, 2008, and 2010, the most common fraud category was lost or stolen cards, but counterfeiting has risen sharply since 2006, and by 2010 its share of total PIN debit fraud was close to that of lost or stolen cards. Lost or stolen cards accounted for 59 percent of PIN debit fraud in 2006 but fell to 49 percent by 2010, while counterfeiting's share rose from 21 percent to 44 percent. IMOTO transactions accounted for only a minor share of PIN debit fraud throughout the period.[5]

Chart 1

SHARES OF ATM AND DEBIT CARD FRAUD BY METHOD OF COMPROMISE



Source: American Bankers Association 2007, 2009, 2011.
Note: The survey question asked respondents to report the method by which fraudsters committed card payment fraud. The survey included 176 commercial bank participants for 2006 and 170 for 2008. For 2010, the survey included 117 full participants and 68 participants who completed an abridged version of the survey.
IMOTO: Transaction by Internet, mail order, or telephone order.
Other includes card not received for 2010.

Card issuers employ a variety of techniques to prevent payment fraud. A decision to approve any card transaction will typically require that the transaction conform to certain preset parameters and comply with a number of rules, such as limits on transaction size. These "decision rules" are used in combination with "transaction screening" methods for identifying transactions that have a high likelihood of being fraudulent. Finally, issuers and merchants both take steps in an "authentication" process aimed at verifying the legitimacy of the cardholder and card. Card issuers conduct some steps in the authentication process remotely while relying on merchants to conduct other steps at the location of the transaction. The text box on the following page provides more detail on the use of decision rules, transaction screening, and authentication protocols to combat fraud.

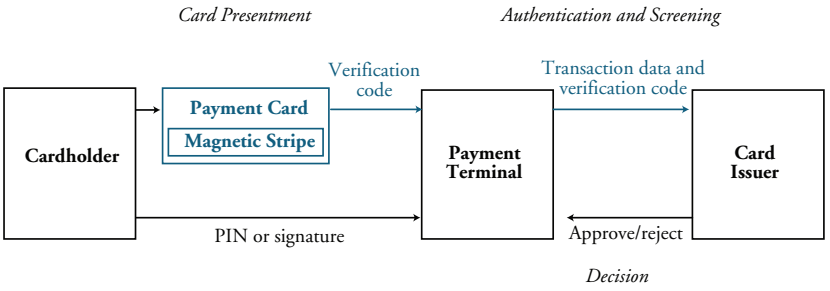
The transmission of encrypted information from a card payment terminal to a card issuer is a key part of the authentication process. Using cryptographic techniques, card issuers write verification codes into the magnetic stripe of each card they manufacture. When a cardholder swipes a magnetic-stripe payment card at a payment terminal, the terminal transmits the verification code to the issuer. The issuer reads the code to be sure it is consistent with the card account number and its expiration date. Any inconsistency may lead the issuer to suspect fraud and decline the transaction. Verification codes thus give merchants and issuers some degree of assurance that the card and cardholder are legitimate.

In the United States, almost all card payment terminals have live telecommunication connections to card issuers, allowing real-time authentication.[6] The initiation of a card payment proceeds in three stages: card presentment, authentication and screening, and the final decision to approve or reject.[7] Figure 1 illustrates these stages and depicts the flow of information involved in single magnetic-stripe card payment. Step-by-step details of the initiation of card payments and the role of authentication are provided in the Appendix.

The vulnerabilities of magnetic-stripe cards

Vulnerabilities in the authentication protocols of magnetic stripe cards—particularly the static nature of their verification codes, which do not change from transaction to transaction—can be exploited in

Figure 1
INITIATION OF MAGNETIC-STRIPE CARD PAYMENTS



diverse ways to send false signals to card issuers. Methods include counterfeiting, signature forgery, PIN harvesting, the use of lost or stolen cards for IMOTO transactions, and data theft.

Counterfeiting a magnetic-stripe card is far easier than counterfeiting a computer-chip card. With the correct data and equipment, fraudsters can create counterfeit magnetic-stripe cards and use them carefully to avoid standing out in a transaction screening process. A relatively simple method for making counterfeit magnetic-stripe cards requires only a computer and a device that can read cards' magnetic stripes and also "write" on them. The equipment is used with an existing card to encode the magnetic stripe with stolen data from another card. The emergence of prepaid gift cards facilitates re-encoding because the cards do not carry the name of the cardholder, thus eliminating a piece of information that is otherwise useful for authentication (Acohido and Swartz). Counterfeiting a new magnetic-stripe payment card with the use of stolen data is more difficult because it requires embossing equipment and blank cards. Nevertheless, motivated fraudsters can find the equipment and supplies they need (Roberts).[8] Whether using a re-encoded or newly created payment card, fraudsters can make a given transaction appear legitimate by "replaying" the static card data.

Signature-authorized transactions can be accomplished by forging the legitimate cardholder's signature, which can usually be found on the back of a lost or stolen card. Issuers must rely on cashiers to reject forged signatures on card payments.[9]

PIN transactions are less prone to fraud because PINs are normally kept secret. However, PINs can be harvested through methods ranging

STRATEGIES TO GUARD AGAINST CARD PAYMENT FRAUD

Card issuers and merchants guard against fraud with a combination of three strategies: decision rules, transaction screening, and authentication.

Decision rules help limit losses in cases where illegitimate transactions are approved as a result of successful fraud. The magnetic stripe on payment cards contains parameters for rules enforced at the payment terminal. For example, rules determining requirements for payment approval, known as "floor limits," are encoded on the card and enforced at the payment terminal (Anderson 2008c). Payment approval systems use automated computer systems. A card issuer might operate the computer system or may outsource its operation to a payment processing intermediary. Low-value transactions may not require issuer approval. A payment-processing intermediary might approve mid-value transactions. Only the issuer would approve high-value transactions. The rules allow automatic approval on lower-value transactions to provide flexibility for various kinds of transactions such as those for parking fees or for mass transit tickets. Other rules set maximum values for any single transaction, determine whether a signature or PIN is required for authorization, and dictate whether international transactions are allowed.

Transaction screening is aimed at identifying transactions that are likely to be fraudulent. The most basic step in transaction screening is for a card issuer to consult records to ensure a payment card and account are both active. The issuer may also enforce a maximum number and maximum value of daily transactions. Advance screening methods seek to detect patterns suggestive of fraud and assign scores indicating the estimated probability that a given request for transaction approval is fraudulent. One method analyzes purchase transactions that are at high risk for fraud, such as purchases of electronic equipment, liquor, gasoline, out-of-country transactions, and IMOTO transactions (Anderson 2008c). Another method analyzes individual transactions to identify those that are out of character for the cardholder and thus seem more likely to be fraudulent. Transaction screening typically involves a computing technique known as "neural networking."

Authentication involves processes designed to verify the legitimacy of both cardholders and the payment cards they present. Issuers conduct their authentication processes remotely while relying on merchants to conduct some authentication processes at the location where payment is made. When a customer presents a payment card to a merchant, the merchant regards possession of the card as verification that the customer owns the card account and can legitimately authorize a payment. For a signature card payment, the merchant can do more to authenticate the cardholder by comparing the signature on the payment terminal with the signature on the back of the card. The merchant authenticates the card by verifying special attributes on the card to rule out counterfeits. The card may include attributes that counterfeiters find hard to

duplicate, such as an elaborate brand logo or a hologram, or information that is repeated on the card, such as elements of the card's account number embossed on the front and printed on the back of the card (MasterCard). Issuers also rely on merchants to screen for counterfeit cards. The PIN authenticates the cardholder in a PIN debit or an ATM transaction, but the issuer relies on the merchant to authenticate the cardholder in a signature debit or credit card transaction.

Authentication efforts by issuers involve the use of cryptographic card authentication codes to authenticate payment cards. Computer-chip payment cards improve issuers' capacity to authenticate payment cards by producing a more effective, secure kind of authentication code in a process known as "dynamic data authentication." The Appendix provides details of the card payment approval process for both magnetic-stripe and computer-chip payment cards.

from "shoulder surfing" by a cashier to more high-tech methods, such as employing fake PIN pads, clandestine video cameras, or tampered payment terminals. In one 2010 case, Las Vegas police arrested a suspect for installing devices on gas pumps to obtain data from more than 13,000 credit and debit cards (Payments Source). The suspect allegedly used the data to re-encode existing payment cards and committed fraud valued at more than $500,000. In another 2012 case, a retail chain found an estimated 90 tampered card terminals that captured both card data and PINs (Digital Transactions News 2012a).

Similarly, imposters can commit payment fraud through IMOTO transactions with lost or stolen cards. Consumers complete transactions at an Internet site by entering card information into appropriate data fields. Merchants and issuers can find it difficult to know whether the card information is legitimate because the merchant cannot see the payment card. Similar difficulties occur if the transaction is over the telephone or by mail order. To fight IMOTO fraud, issuers print a card verification code on the back of the card. The issuer can use the code to authenticate the card and gain additional assurance that the customer has it in his or her possession. However, this layer of security will work only if the IMOTO merchant requires the verification code, which is not always the case.[10]

Data breaches are a key source for stolen card data. Fraudsters can use the data to create counterfeit cards and to conduct IMOTO transactions. The web site Data Loss Database reports that payment card

Table 2

SOURCE OF COMPROMISED DATA USED FOR PAYMENT CARD FRAUD

Financial Institutions, 2008 and 2010

Year	Source of Compromised Data		
	Data Breaches	Phishing or Spoofing	Skimming
	Percent		
2008	43	22	15
2010	31	29	35

Source: American Bankers Association 2009, 2011.
Note: Survey respondents were asked to report the extent to which losses their banks had incurred from card payment fraud were a result of information obtained by data breaches, phishing or spoofing, or skimming. In 2008, 170 commercial banks were surveyed. For 2010, survey respondents included 117 full participants and 68 participants who completed an abridged version of the survey.

data was exposed in 954 of the 6,784 publicly announced data breaches since 2003.[11] In the largest U.S. data breach, hackers installed software on the computer system of a payment processor that exposed data from 130 million payment cards in 2009 (DatalossDB). The breach affected at least 670 banks, with at least 197 re-issuing many of their payment cards.[12] In addition to the costs of reissuing cards, banks that suffer such breaches must bear the expense of notifying customers, the monetary losses from the use of card information to commit payment fraud, the legal costs of resolution, and the cost of a damaged reputation (Wicks). Additional methods leading to breached data, aside from hacking, include the theft of computers, social engineering or scams, website searches, and documents retrieved from trash containers.

Stolen data can also come from sources other than data breaches. Consumers sometimes reveal payment card information in response to fake emails (phishing) or fake websites (spoofing).[13] Fraudsters also install disguised magnetic-stripe card readers on gas pumps, ATMs and other locations, "skim" card data as cardholders present their cards, and collect that data for later use (Nikias).

Depository institutions report that data breaches were the leading source of compromised data used for payment fraud in 2008, accounting for 43 percent of fraud losses tied to stolen data. However, this share declined to 31 percent by 2010 as other sources of compromised data increased (Table 2). Over this period, data skimming grew to be the leading source of compromised data, rising from 15 percent in 2008 to 35 percent in 2010. Phishing and spoofing accounted for 22 percent

of compromised data in 2008 and 29 percent in 2010. Another survey of debit card issuers found that 94 percent of respondents had been affected by at least one data breach (Pulse Network). Among the surveyed debit card issuers, data breaches had exposed the data of 31 percent of their debit cards, on average.

II. THE ADOPTION OF COMPUTER-CHIP CARDS

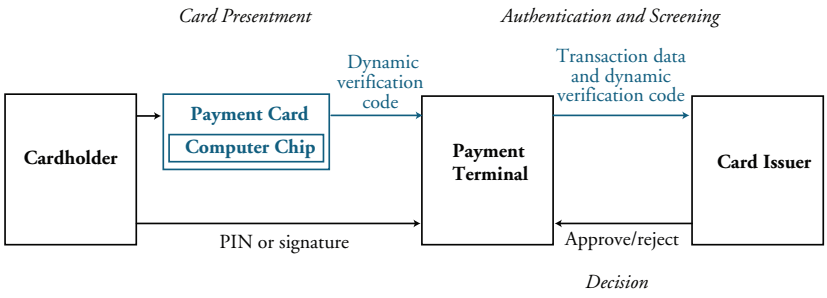
Computer-chip payment cards are replacing magnetic-stripe cards in nearly all developed countries in the world. The new cards comply with the Europay, MasterCard, and Visa (EMV) specifications, which define methods of processing and security features for computer-chip cards issued by MasterCard, Visa, JCB, and American Express.[14] Adherence to the specifications ensures interoperability wherever issuers adopt EMV-based cards and wherever merchants accept them. In 2011, 44.7 percent of payment cards and 76.7 percent of payment terminals worldwide complied with the EMV specifications (EMVCo).[15] All EMV payment cards have computer chips with the capacity to use encryption protocols.

The advantages of computer-chip cards

Cards with an imbedded computer chip used for payments have many more capabilities than magnetic-stripe cards (Smart Card Alliance). Computer-chip cards are much harder to counterfeit, can protect information stored on the chip more effectively, and can defend against unauthorized intrusions. A computer-chip card can use encryption to protect sensitive data, can authenticate messages that it receives, and can send messages to issuers that enable the issuers to authenticate transactions more reliably than they can with magnetic stripe cards.[16] Computer-chip payment cards also can modify payment data for security purposes.

The capacity of the computer chip on a payment card to encrypt data makes possible a process of "dynamic data authentication."[17] Unlike magnetic-stripe cards, which bear static verification codes that do not change from one transaction to another, computer-chip payment cards can customize a distinct verification code for each transaction.[18] One type of card capable of dynamic data authentication

Figure 2
INITIATION OF COMPUTER-CHIP CARD PAYMENTS



is already in use in the United States. Known as contactless cards, these cards have embedded computer chips that can transfer transaction data via radio signal if the cardholder passes the card close to a payment terminal. The chips on these cards use secret encryption keys and algorithms to produce changing verification codes for use in authentication (Smart Card Alliance).

Figure 2 illustrates the three stages of processing a computer-chip card payment and the associated information flows. The computer chip generates a dynamic verification code by adding a transaction-specific number to the other card data, ensuring that the verification code changes from transaction to transaction.

Changing the verification code used for authentication in payments has a similar benefit to requiring computer users to change their passwords regularly. If a hacker steals a password, but users change passwords regularly, the window within which the hacker can take advantage of the stolen password is small. If a hacker steals payment card data that produces dynamic verification codes, the hacker's ability to use the card data for fraud is similarly limited.[19]

Dynamic authentication helps prevent fraud at the transaction level.[20] It stops fraudsters from making fraudulent payments merely by replaying the data from a payment card that uses the same verification code for every transaction. Under a dynamic data authentication protocol, such an approach would be unsuccessful because fraudsters cannot generate the ever-changing verification codes needed for successive transactions.

Dynamic data authentication also has a general effect that helps reduce all methods of card payment fraud. The weak authentication of magnetic-stripe payment cards provides criminals with incentive to obtain card data for use in making fraudulent payments. The stronger authentication processes made possible by computer-chip cards, however, reduce criminals' incentives to obtain card data. As a result, data breaches, phishing, and social engineering attacks are all likely to decline as computer-chip cards become widespread.

The recent experiences of France, the Netherlands, and the United Kingdom as they shifted from magnetic-stripe to computer-chip payment cards reveal the benefits of adopting computer-chip payment cards and the challenges posed when fraud shifts to payments with relatively weak authentication protocols.

Adoption in France

France began to use computer-chip payment cards in 1992 and upgraded to the EMV specification between 2001 and 2008. Initially, French issuers used cards with static data authentication. Fraudsters learned how to reprogram the card so that some transactions would pass the approval process with any PIN. (Given the capacity of such reprogrammed cards to obtain approvals, they became known as "Yes" cards.)[21] French issuers responded by switching to dynamic data authentication cards from 2005 to 2008. As a result, counterfeit card fraud declined substantially in 2006. Fraud on lost or stolen cards also fell.

Subsequently, however, French fraudsters simply turned their focus to types of transactions that involve weaker authentication methods—a trend that may have implications for the future of payment card fraud in the United States. By 2010, fraud on IMOTO transactions was the top source of card payment fraud in France (Observatory for Payment Card Security 2011). The fraud rate on IMOTO transactions increased yet further in 2011, accounting for 61 percent of the total value of card payment fraud in France, but only 8.4 percent of the total value of all French card payments. As a preventive measure, French authorities now encourage Internet merchants to adopt an enhanced type of IMOTO transaction authentication called 3D secure.[22] In 3D secure payments, a cardholder registers a payment card with the issuer and creates a PIN, which the cardholder then uses in an Internet purchase. Cardholder

authentication is much stronger in 3D secure transactions because the cardholder must use the PIN.

Although the fraud loss rate on card payments in France drifted downward for several years and is still relatively low, it ticked up in 2011 for "card-present" transactions, both for purchases and for withdrawals from bank accounts. (Card-present transactions are those wherein the card is actually present at the location of payment, as opposed to IMOTO transactions where the card is not present.) Authorities attribute the rise to an increase in theft of cards wherein the thief also obtains a PIN.

Adoption in the Netherlands

In 2006, along with all members of the Single European Payments Area (SEPA), the Netherlands was mandated to migrate to EMV payment cards.[23] The Netherlands began the switch to EMV cards and terminals in 2007 (Currence 2007). Although the switch was within the 2010 target completion date for the EMV transition, the Netherlands retained magnetic-stripe cards longer than most other SEPA countries.[24]

Criminals took advantage of the magnetic-stripe terminals to skim card data and create counterfeit cards. In 2011, there were 555 successful skimming attacks on payment terminals, up from 176 in 2010. Nearly half of the successful payment terminal skimming attacks occurred in unattended parking lots. Another 182 successful skimming attacks occurred on ATM machines. Losses due to card skimming rose from €2.5 million ($3.1 million)in 2005 to over €35 million ($49 million) in 2009. Losses dropped to €20 million ($27 million) in 2010 but rebounded to nearly €40 million ($56 million) in 2011 (Currence 2011).

The Netherlands has now completed the migration to EMV cards and terminals but remains exposed to skimming attacks because EMV payment cards often also have magnetic stripes and some locations still accept magnetic-stripe cards. Although discussions have been held in Europe on removing magnetic stripes from payment cards, practical difficulties—relating to equipment compatibility, the speed of transactions, and the need for fallback options when EMV is unavailable—have delayed their elimination (Observatory for Payment Card Security 2010).

Adoption in the United Kingdom

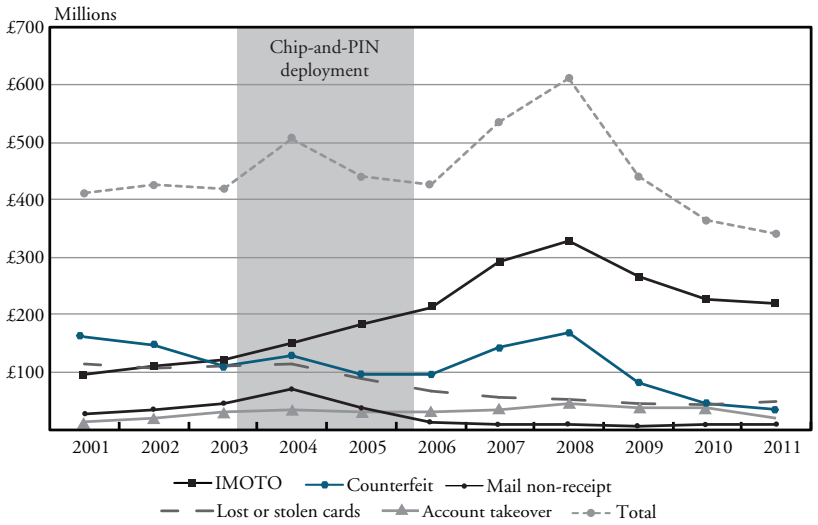
A phased, national rollout of EMV payment cards in the United Kingdom began in October 2003, with a targeted completion date of February 2006. EMV payment cards in the UK are called "chip-and-PIN" cards because all transactions (purchases and withdrawals) require a PIN. The benefits of EMV payment cards were apparent as early as 2005 when fraud losses due to lost or stolen cards began to decline (Chart 2). Both the added fraud protection due to the computer chip and the required use of a PIN for transactions successfully limited the ability of anyone who possessed a lost or stolen card to create a fraudulent payment.

Payment fraud soon migrated to channels in the UK with weaker authentication, such as cards still using magnetic stripes and IMOTO purchases.[25] For backward compatibility, during a transition period, new EMV payment cards typically had both computer chips and magnetic stripes. Fraudsters could then make counterfeit magnetic-stripe payment cards and use them wherever merchants or ATMs still accepted the cards, especially outside the UK. As a result, fraud losses on counterfeit cards in the UK grew from £97 million ($176 million) in 2005 to £170 million ($312 million) in 2008. The move to EMV payment cards also left authentication unchanged for IMOTO transactions, making them another attractive outlet for fraudsters. Fraud on IMOTO transactions grew rapidly, from £183 million ($333 million) in 2005 to £328 million ($602 million) in 2008.

After 2008, fraud losses with counterfeit cards and on IMOTO transactions declined. The decline was due to two factors. First, more merchants and ATMs on the European mainland had converted by that time to accept EMV payment cards, so fraudsters with counterfeit magnetic-stripe cards could no longer easily find locations where magnetic-stripe cards were accepted, merely by crossing borders. Second, increasingly, merchants in the UK were adopting 3D secure systems for their IMOTO transactions. In 2007, only 25 percent of respondents to a survey of UK Internet merchants reported that they accepted 3D secure payments, but the same survey found at least 59 percent of respondents accepted 3D secure in 2011 (Cybersource 2008, 2012b).[26] Total fraud losses on payment cards in the UK fell significantly, from a

Chart 2

VALUE OF LOSSES DUE TO CARD PAYMENT FRAUD IN THE UNITED KINGDOM



Source: UK Cards Association 2012a.

peak of £610 million ($1,120 million) in 2008 to £341 million ($547 million) in 2011.

The experiences with computer-chip payment cards in France, the Netherlands, and the United Kingdom show that the ability to deter card payment fraud depends not only on the use of computer chips but also on other key factors. Computer chips proved their value for limiting fraud on counterfeit cards. However, computer-chip cards that still allowed the use of static data authentication were still vulnerable to attacks. Other significant declines in fraud were independent from the adoption of computer chips, resulting instead from the elimination of the magnetic stripe and improved authentication methods for IMOTO transactions.

III. IMPLICATIONS FOR THE UNITED STATES OF FRAUD TRENDS IN EUROPE

American Express, Discover, MasterCard, and Visa have recently announced plans to switch to EMV-compliant, computer-chip payment cards in the United States (Digital Transactions News 2012b). Issuers that use these card brands will release EMV payment cards over

the next few years. The card brands are also creating strong incentives for merchants to begin accepting the new cards by modifying liability rules for fraudulent card payments. Liability for fraudulent payments, which falls to the card issuer in an approved, card-present transaction, will shift to the party in the payment process (issuer, processor or merchant) that provides the least security.[27] The current schedule shifts fraud liability on October 1, 2015.

If the use of EMV payment cards in the United States leads to a fraud loss pattern similar to the patterns seen in France, the Netherlands, and the UK, then U.S. fraud losses could fall by as much as 40 percent. In 2009, the loss rate for the United States on the value of card purchase transactions was an estimated 0.110 percent (Table 3). France has used EMV payment cards for many years, and in 2009, its fraud loss rate was 0.067 percent, or 39 percent lower than the U.S. loss rate. The UK deadline for the switch to EMV payment cards was April 2006, and by 2009 its fraud loss rate was 0.097 percent. The loss rate for the UK continued to fall to 0.065 percent in 2011, or 41 percent lower than the 2009 loss rate on payment cards in the United States.[28]

The experiences of other countries may illustrate the short-term impact that EMV payment cards could have on fraud in the United States. EMV payment cards will likely succeed in cutting off some methods of card payment fraud but fraud will also shift to other types of card payment with relatively weak authentication protocols. Counteracting those shifts may require additional steps. Counterfeit cards are a leading, and increasing, method of committing fraud on debit cards in the United States. The adoption of computer-chip payment cards will help to reduce counterfeiting. But as long as card issuers maintain the magnetic-stripe, either alone on payment cards or along with a computer chip, they will continue to be a significant and possibly increasing source of counterfeit card fraud.

Fraud for card-present transactions on lost or stolen cards may stay the same or even potentially increase. Many countries that use EMV payment cards do not allow cardholder authentication with signatures. Issuers in the United States, however, appear likely to continue to allow signature authorization on EMV debit and credit card transactions (Heun; Punch). As a result, fraud on lost or stolen cards may not decline in the United States. Fraud may even rise as fraudsters,

Table 3

INTERNATIONAL COMPARISON OF LOSS RATES ON DEBIT AND CREDIT CARD

Purchase Transactions 2009

Location of card issuer	Loss per Value of Transactions (percent)
United States	0.110[1]
United Kingdom	0.097
France	0.067

[1]Average fraud loss is $3.45 billion in losses divided by $3.13 trillion transactions, which equals 0.11 percent. Similar calculations apply to the United Kingdom and France.
Sources: United States: Board of Governors and Federal Reserve System (see Table 1). United Kingdom: UK Cards Association 2012a, 2012b. France: Observatory for Payments Card Security 2009.
Note: Losses are for card issuers in each country on both domestic and foreign purchase transactions. The United Kingdom loss rate includes a small number of foreign ATM withdrawals.

unable to commit fraud on counterfeit cards, begin to target payments with relatively weak security, such as transactions that allow signature authorization.[29] Fraudsters may put more effort into stealing computer-chip payment cards, knowing that they may be able to commit a few fraudulent transactions using a forged signature before issuers cut off use of the card.

For similar reasons, fraud in IMOTO transactions in the United States can be expected to increase. Stronger authentication for Internet transactions, such as 3D secure systems, could limit this method of payment fraud. Alternatively, a secure computer-chip payment card reader attached to a customer's computer could make use of the card's computer chip and thus obtain the full advantage of the chip's dynamic data authentication capacity. Concerns over costs and customer convenience, however, make it is unclear whether issuers will support these options.

Fraudsters' cost-benefit calculations for exploiting other flaws in the EMV specifications will also change. Computer experts have uncovered potential weaknesses on EMV payment cards (Anderson 2012c). For example, fraudsters could tap into the middle of a payment communication link, alter and divert the payment message to a confederate, and fool the payment approval system into accepting a fraudulent payment (Murdoch). These exploits are prototypes that are difficult to implement, and there are no reports of their use other than as demonstrations. However, the payoff to payment fraud is high enough that

fraudsters are likely to research these alternatives and possibly develop technology to make them practical. In the process, they may find other weaknesses of which the industry is unaware today.

The experience of countries that have adopted computer-chip payment cards shows that EMV payment cards offer capabilities for strengthening authentication and preventing fraud. The degree of payoff from adopting the cards only emerges over time, however, because authentication methods tend to evolve and improve during a transition period. Still, some fraud will migrate to payments with weak authentication capacities, and card issuers will need countermeasures to improve authentication.

IV. CONCLUSION

As the United States begins its transition to computer-chip payment cards, the country will reap the benefits of dynamic data authentication and improved resistance to counterfeiting. Some sources of payment fraud, such as counterfeit cards, will decrease. However, experience also shows that other sources of fraud are likely to increase. Thus the prospects for reducing overall card payment fraud depend on how authorization and authentication protocols are implemented. If weaker authorization protocols continue, such as signatures for card payments rather than PINs, the degree of fraud reduction that can be achieved will be limited. Similarly, unless authentication protocols are improved for IMOTO transactions, such transactions will become a weak link in the defenses against fraud, and IMOTO fraud will likely increase.

The payment industry must also be alert to new forms of fraud as attackers probe for security weaknesses and exploit them. Fraudsters have strong incentives to commit payment fraud and will continue to test security measures and sometimes defeat them. Card issuers, in turn, will need to reevaluate their choices of authorization and authentication methods periodically, as new trends in fraud emerge.

In contrast with many other advanced countries, the United States does not have a comprehensive system for collecting and reporting statistics on payment fraud (Sullivan 2009). Timely information on the sources of fraud allows policymakers and the card payment industry to respond swiftly and effectively to new attacks. The UK system for capturing and monitoring such information was a critical asset enabling the payment card industry there to respond to the new trends in fraud

that emerged during the transition to chip-and-PIN cards. In fact, in the absence of critical information on the sources and types of card payment fraud, efforts aimed at limiting fraud may be misdirected and wasteful. Both regulators and the card payment industry could benefit from mechanisms to measure the levels and sources of fraud and to identify who pays the price—and how much is paid—for the nation's losses from payment card fraud.

APPENDIX
CARD PAYMENT INITIATION, ENCRYPTION, AND MESSAGE AUTHENTICATION CODES

The initiation of card-present payments has three stages: card presentment, authentication and screening, and the decision to approve or reject. Figure A, Panel A illustrates these steps and shows the flow of information for both magnetic-stripe and computer-chip card payments. The processes differ, with computer-chip card payments involving additional steps that enable more effective authentication.

In a standard magnetic-stripe card payment, the cardholder first presents a card to a payment terminal, by swiping the card or inserting it into the terminal. The terminal captures card data from the magnetic stripe, including the card account number (which is known as the primary account number) the cardholder's name, and the expiration date (Observatory for Payment Card Security 2010). The terminal also captures a verification code from the magnetic stripe.[30] The cardholder then authorizes the payment by providing a signature or entering a PIN. In a PIN transaction, the terminal uses its own computer chip to encrypt the PIN (Figure A, Panel B). The terminal adds details about the transaction, such as transaction value and merchant identification data, to the card data and the encrypted PIN. The terminal then sends all of the transaction data to the issuer for authentication and screening.

The issuer authenticates the verification code. The issuer also verifies the account by ensuring that the primary account number, cardholder name, and expiration date match its records, and checks that either sufficient funds are in a debit card account or a credit limit is sufficient on a credit card transaction. The issuer may then screen details of the transaction to determine whether it is at high risk for fraud. If the transaction passes these steps, the issuer will allow the transaction to proceed by returning an approval message to the merchant. If the transaction does not pass any of the steps, the issuer rejects the transaction.

In a computer-chip card payment, the transaction proceeds in a fashion similar to the magnetic-stripe transaction, but the computer chip generates a dynamic verification code by adding information unique to each given transaction—such as a serial number—to other card information. The chip then applies an encryption algorithm to generate a dynamic verification code and sends it to the payment

terminal (Figure A, Panel C). The dynamic verification code (sometimes called a dynamic cryptogram) is added to other payment information and sent to the card issuer.

The dynamic verification code includes the information contained in the verification codes of a magnetic-stripe cards, allowing the issuer to authenticate the transaction by comparing information sent by the terminal to its internal records. But computer-chip authentication is enhanced because the issuer can consult its records to see if any user has previously submitted the exact same dynamic verification code. If not, the issuer knows that the data sent to the issuer for payment approval is not a replay of a previous transaction and thus has additional assurance that the transaction is genuine.

The role of authentication, encryption, and message authentication codes

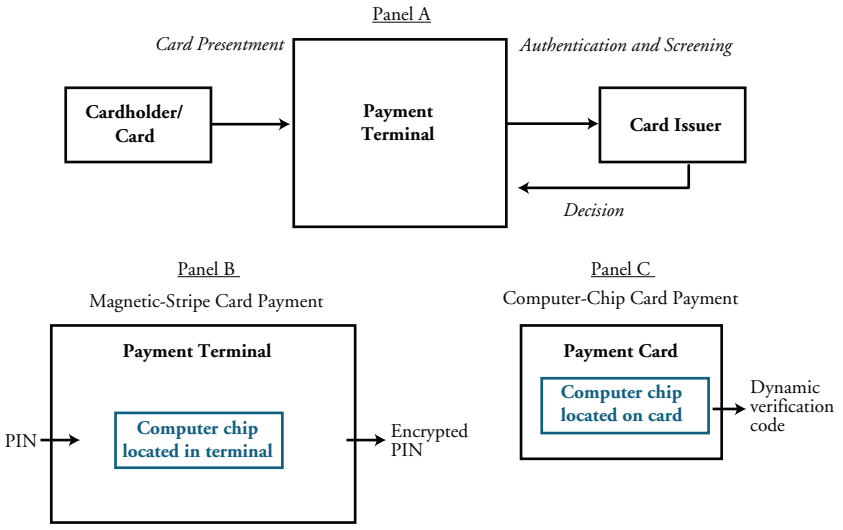
Authentication protocols are crucial for the issuer to trust a given transaction. Both the verification code from a magnetic-stripe payment card and the dynamic verification code from a computer-chip payment card are key components in their respective authentication protocols. In each case, encryption plays a crucial role. The best known purpose of encryption is to keep sensitive information private, but encryption also can be used to help ensure that a message is genuine. The verification codes are examples of "message authentication codes" (MACs), generated by an encryption key and a mathematical process, or algorithm (Anderson 2008b, 2008c). To make this method of authentication work, only the card issuer can have the encryption keys and knowledge of the specific algorithms used to derive the verification codes.[31]

A MAC helps a card issuer make a correct decision to accept or reject a given payment. In a computer-chip card payment, the chip generates a MAC based on the cardholder's primary account number, the card's expiration date, and a serial number or other transaction-unique data. (Anderson 2008b; Smart Card Alliance).[32] The issuer tracks the unique data of the card's transactions and uses them, along with other payment card data from its internal records, to generate a MAC for each transaction. The MAC that the issuer has generated for the given transaction is then compared with the MAC sent by the computer-chip card. If they do not match, the issuer does not approve the transaction (CUNA Mutual Group).

Figure A

INITIATION OF MAGNETIC-STRIPE AND COMPUTER CHIP CARD PAYMENTS

Steps in italics are available with computer-chip payment cards



Card Presentment

1. Cardholder presents card and terminal captures card data (primary account number, cardholder name, expiration date, and security code)
2. Cash register sends purchase information to payment terminal
3. Cardholder enters PIN or signature
4. In a PIN transaction, payment terminal generates encrypted PIN (Panel B)

4a. Computer-chip payment card calculates dynamic verification code, using an encryption algorithm, a symmetric encryption key, and a transaction serial number or other transaction-specific data (Panel C)

4b. Terminal captures dynamic verification code

Authentication and Screening

5. Payment terminal sends card data, merchant ID, transaction value, and static verification code to issuer

5a. Terminal sends a dynamic verification code to issuer

6. Issuer authenticates PIN and card (PIN transaction) or card (signature transaction)

6a. Issuer confirms dynamic verification code is not a duplicate

7. Issuer verifies primary account number, expiration date, cardholder name, and available balance
8. Issuer screens transactions for high risk of fraud

Decision

9. Issuer approves and terminal completes transaction or issuer rejects transaction

ENDNOTES

[1]There is no source of comprehensive information on payment fraud losses in the United States (Sullivan 2009). The estimates in Table 1 rely on Federal Reserve surveys regarding fraud loss rates for debit card payments and retail payment values (Board of Governors 2011; Federal Reserve System 2011). Statistics on methods of compromise are available for PIN-authorized transactions (debit card transactions combined with ATM withdrawals) and signature-authorized debit card transactions, but not for credit cards. For credit cards, however, the distribution of methods of compromise is likely similar to that of signature debit, since both use similar authorization and approval methods. The estimates in Table 1 therefore assume that the loss rate on credit card payments is the same as that on signature-authorized debit card payments.

[2]Another less common method of card payment fraud occurs when an imposter takes over a payment account. An account takeover may occur when a hacker obtains a consumer's user ID and password to access an online banking account and then performs fraudulent transactions. The share of signature and PIN debit fraud due to account takeover was 7 percent or less of all fraudulent transactions, throughout the 2006-2010 period.

[3]In the United States, debit cards may require either a PIN or a signature, ATM withdrawals require a PIN, and credit cards require a signature.

[4]King provides an analysis comparing the security of PIN and signature transactions.

[5]PIN debit is not widely used in IMOTO transactions because more Internet merchants are requiring card verification codes (a 3-digit code on the back of a payment card) which work only for signature debit transactions. In 2011, 79 percent of Internet merchants required the code, up from 66 percent in 2005 (Cybersource, 2007; 2012a). Acculynk provides a service that allows cardholders to enter a PIN for debit transactions on the Internet, but it is in the early stages of adoption.

[6]In the few cases where card transactions occur when telecommunications connection is unavailable, card issuers set a transaction value under which they automatically approve payments despite the lack of connection.

[7]The three-stage process described here applies to "card-present" transactions, wherein the actual card is present at the location of payment, and not to IMOTO transactions where the card is not present.

[8]Physical elements of payment cards such as complex graphics and holograms are added to help deter counterfeiting.

[9]Merchants can train their cashiers to spot forgeries. See for example, "Is This Signature Forged?" Bankers Online (*www.bankersonline.com/articles/bhv01n11/bhv01n11a7.html*). Cashiers, however, can be mistaken or careless (John Hargrove, "The Credit Card Prank," *http://www.zug.com/pranks/credit/*).

[10]Seventy-nine percent of respondents to a survey of large online merchants ask for the card verification code (Cybersource 2012a). In contrast with card-present transactions, the merchant does not get a guaranteed payment when the card is not present. Merchants deploy a variety of tools to avoid card payment fraud, including confirmation of card verification codes, verification of cardholders' addresses, transaction history tracking, and tracking of customers for histories of fraud.

[11]As of January 17, 2013. See *datalossdb.org*.

[12]The breach occurred at Heartland Payments Systems. These statistics are based on a list of affected banks on the Bank Info Security website (*www.bankinfosecurity.com/articles.php?art_id=1200*, accessed Feb. 23, 2012). The website speculates that the actual number of banks affected is closer to 3,000.

[13]In a recent example, scammers produced high-quality replicas of a mobile phone provider's email alerts for its customers' monthly bills and induced some recipients to reveal sensitive payment data (Goessl).

[14]An organization called EMVCo manages the EMV specifications (see *http://www.emvco.com/*). Formed in 1999, EMVCo is currently owned by American Express, JCB, MasterCard and Visa. EMVCo's current ownership reflects the acquisition of Europay by MasterCard in 2002 and the additions of JCB (2004) and American Express (2009). EMVCo also administers a testing and approval process and oversees procedures for confirming compliance with the EMV specification.

[15]Not all countries have highly reliable telecommunications systems. The EMV specification allows card and cardholder authentication without an online connection using an interaction between the card and terminal. This article does not discuss offline authentication because the U.S. telecommunications system is highly reliable and allows nearly all card transactions to use online authentication.

[16]The technology involves symmetric encryption keys (a key on the chip that is only known to the card issuer) and asymmetric encryption/digital certificates to confirm essential identities such as the issuer and the brand of the card.

[17]Not all EMV payment cards use dynamic data authentication. Dynamic data authentication requires more capable and costly computer chips.

[18]Dynamic authentication codes are related to a type of message element that computer scientists call a "nonce" ("number used once") that is used only once (Anderson 2008a). If an authentication code changes from transaction to transaction, then the issuer has information that tells it the code is "fresh" or recently created. Security protocols include dynamic authentication specifically to prevent replay attacks.

[19]A transaction with this card may be processed, however, if communications or computer systems are unavailable and the payment approval protocol defaults merely to a floor limit for offline authentication.

[20]Dynamic authentication requires a computer chip but the chip does not necessarily need to reside on the payment card. A computer chip on a payment

terminal could add a dynamic verification code to a payment approval request for a magnetic-stripe card payment (PRNewswire; see also *www.magtek.com/index.asp*).

[21]These cards work only if payment authentication takes place offline and where authentication of the card uses static data (Anderson 2008c). Visa and MasterCard now require new EMV payment cards in Europe to use dynamic authentication (DDA Authentication in Europe).

[22]IMOTO card payments are not normally guaranteed, but merchants do get a guarantee if they use 3D secure (Bustos). Visa and MasterCard call their 3D secure systems, respectively, Verified by Visa and SecureCode.

[23]The mandate became official in 2006 with the adoption of Version 2 of the European Payments Council's "SEPA Card Framework" (European Payments Council).

[24]Several European countries began adopting EMV payment cards prior to 2006.

[25]Moore and Anderson review recent research on the strategic interaction of defense and attack in data security.

[26]The 25 percent acceptance rate for 2007 was for Internet merchants who accepted either Verified by Visa or SecureCode, two brands of 3D secure payment. For 2011, 59 percent of respondents accepted SecureCode, and 65 percent accepted Verified by Visa.

[27]Merchants also have incentives to adopt EMV card payment prior to this deadline. Merchants can avoid some of the costs of complying with data security standards for payment cards if they accept a minimum threshold of EMV card transactions. For example, the threshold for Visa is 75 percent of transactions processed on EMV compliant terminals (Digital Transactions News 2012c). Card companies have also set a 2013 deadline for processors to be capable of processing EMV payment cards.

[28]These figures on UK loss rates are not shown in Table 3. UK card issuers lost £312 million on £475 billion worth of card purchases and £7 billion in overseas cash withdrawals for 2011, a loss rate of 0.065 percent (U.K. Cards Association 2012a, 2012b).

[29]It is unclear how dynamic authentication will deter fraud on lost or stolen cards any more effectively than static authentication because the online authorization system in the United States allows issuers to refuse magnetic-stripe card payments as soon as they become aware that a card is lost or stolen.

[30]For a transaction requiring a PIN, the terminal captures a PIN verification code, also known as the PIN verification key indicator or PIN verification value. For transactions requiring a signature, the terminal captures a card verification code (also known as the card verification value).

Issuers added the PIN verification code to the magnetic stripe in the early 1990s after a flood of payment card fraud through signature forgeries (Anderson 2008c).

[31]For a PIN payment card, an algorithm encrypts the combined PIN, primary account number and expiration date to generate the PIN verification

code. For a signature payment card, an algorithm encrypts only the combined primary account number and expiration date to generate the card verification code.

In a PIN transaction, both the PIN and the PIN verification code help to secure the payment. The cardholder knows the PIN and keeps it secret to prevent unauthorized use by others. The card issuer knows the PIN verification code and knows the encryption key and algorithm that produced the code, which allows the issuer to verify the PIN and the payment card. Similarly, for a signature payment card, the issuer can verify the payment card. One reason that signature card payments are more prone to fraud is the online authorization systems can only verify the card, while in a PIN payment card, it can verify both the card and the PIN.

[32]One reason the MAC is used instead of simply encrypting and sending the entire message is that size of encrypted text in digital form is much larger than the plain text message. If the text is not sensitive, so that the only question is the integrity of the message, then communications costs can be lower if the size of the digital messages is smaller by sending the MAC along with the plain text message.

REFERENCES

Acohido, Byron and Jon Swartz. 2007. "Thieves Turn Simple Strip Into Cutting-edge Tool," USA Today, July 31. Available online at: *www.usatoday.com/tech/news/computersecurity/infotheft/2007-07-31-gift-cards_N.htm.*

American Bankers Association. 2007. "Deposit Account Fraud Survey Report."

_____. 2009. "Deposit Account Fraud Survey Report."

_____. 2011. "Deposit Account Fraud Survey Report."

Anderson, Ross. 2008a. "Protocols," Security Engineering. Second Edition. New York: John Wiley and Sons, pp. 63-92.

_____. 2008b. "Cryptography," Security Engineering. Second Edition. New York: John Wiley and Sons, pp. 129-184.

_____. 2008c. "Banks and Bookkeeping," Security Engineering. Second Edition. New York: John Wiley and Sons, pp. 313-363.

Board of Governors. 2011. "2009 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions." Federal Reserve System.

Bustos, Linda. 2011. "Who Needs 3D Secure? Verified By Visa and MasterCard SecureCode Examined." Get Elastic website, March 7th, 2011. Available online at: *www.getelastic.com/who-needs-3d-secure-verified-by-visa-and-mastercard-securecode-examined.*

CUNA Mutual Group. 2006. "Plastic Card Security Practices." Available online at: *www.nebrcul.org/files/nebraska /1/file/CU%20Statistics/Plastic%20Card%20Security.pdf*

Currence. 2007. "Annual Report."

_____. 2011. "Annual Report."

Cybersource. 2007. "Online Fraud Report." Eighth Edition.

_____. 2008. "U.K. Online Fraud Report." Fourth Edition.

_____. 2012a. "Online Fraud Report." Thirteenth Edition.

_____. 2012b. "U.K. Online Fraud Report." Eighth Edition.

DatalossDB. 2009. "Malicious Software Hack Compromises Unknown Number of Credit Cards at Fifth Largest Credit Card Processor." Available online at: *www.datalossdb.org/incidents/1518-malicious-software-hack-compromises-unknown-number-of-credit-cards-at-fifth-largest-credit-card-processor.*

"DDA Authentication in Europe." 2010. Giesecke & Devrient web site. Available online at: *www.gi-de.com/gd _media/media/documents/complementary_material/mobile_security_2/DDA_Authentication_in_Europe.pdf*

Digital Transactions News. 2012a. "Visa Unveils Chip Services As Its U.S. EMV Card Base Crosses the 1 Million Threshold." Available online at: *www.digitaltransactions.net/news/story/3422.*

_____. 2012b. "Discover Releases an EMV Plan That Echoes Key Deadlines from Visa, MasterCard." Available online at: *www.digitaltransactions.net/news/story/3462.*

_____. 2012c. "PCI Waiver Expected To Spur Merchant Adoption of EMV Terminals." Available online at: *www.digitaltransactions.net/news/story/3730.*

EMVCo. 2012. "Latest EMVCo Figures Reveal Continues Market Adoption of EMV Technology." Press Release, May 8. Available online at: *www.emvco.com.*

European Payments Council. 2009. "SEPA Card Framework," Version 2.1.

Federal Reserve Board. 2012. "Average Debit Card Interchange Fee by Payment Card Network," available at: *http://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm.*

Federal Reserve System. 2011. "The 2010 Federal Reserve Payments Study." April 5.

Goessl, Leigh. 2012. "Email scam: Fake Verizon bills duping customers." *Digital Journal.* May 17. Available online at: *www.digitaljournal.com/article/325056.*

Heun, David. 2012. "MC: Pick Any Chip-Card Security You Want, as Long as It's PIN." American Banker. February 2. Available online at: *www.americanbanker.com/issues/177_23/mastercard-visa-emv-liability-shift-chip-and-pin-1046286-1.html.*

King, Douglas A. 2012. "PIN Authentication Versus Signature Authentication." Portals and Rails blog, Federal Reserve Bank of Atlanta (January 23). Available online at: *portalsandrails.frbatlanta.org/2012/01/pin-authentication-vs-signature-authentication.html*

MasterCard. 2012. "MasterCard Card Identification Features." Available online at: *www.mastercard.com/uk/merchant/en/security/datasecurityrules/card_id_sec_features.html*

Moore, Tyler and Ross Anderson. 2012. "Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research." Forthcoming in M. Peitz and J. Waldfogel, eds., *The Oxford Handbook of the Digital Economy*. Oxford University Press.

Murdoch, Steven J. 2007. "Chip & PIN Relay Attacks." Light Blue Touchpaper website." February 6. Available online at: *www.lightbluetouchpaper.org/2007/02/06/chip-pin-relay-attacks/*

Nikias, Maria. 2012. "Thieves Target Gas Pumps to Skim Credit, Debit Cards," ABC News Website. March 15. Available online at: *abcnews.go.com/blogs/headlines/2012/03/thieves-target-gas-pumps-to-skim-credit-debit-cards/*

Nilson Report. 2012a. "Purchase Volume at Merchants in the U.S." Issue 988. February.

_____. 2012b. "Purchase Volume at Merchants on U.S. General Purpose Cards." Issue 994. May.

Observatory for Payment Card Security. 2009. "Appendix D: Statistics." *Annual Report*. Bank of France, pp. 65-68.

_____. 2010. "Security Issues Linked to Developments in French and European Card Payment Schemes." *Annual Report.* Bank of France, pp. 67-76.

_____. 2011. "Fraud Statistics for 2011." *Annual Report.* Bank of France, pp. 21-28.

Payments Source. 2010. "Nearly 14,000 Cards Skimmed In Alleged Scheme." Available online at: *www.paymentssource.com/news/nearly-cards-skimmed-in-alleged-scheme-3003385-1.html.*

PRNewswire. 2012. "Viableware and MagTek Partner to Protect Card Payments Made By Restaurant Guests Using RAIL Payment Platform from Viableware." June 27. Available online at: *www.prnewswire.com/news-releases/viableware-and-magtek-partner-to-protect-card-payments-made-by-restaurant-guests-using-rail-payment-platform-from-viableware-160499645.html*

Pulse Network. 2011. "Debit Issuer Study: Executive Summary."

Punch, Linda. 2011. "Security: Why PINs Need Performance-Enhancing Technology." *Digital Transactions Magazine.* September.

Roberts, Ed. 2011. "Jail Time Given To Person Convicted In Card-Skimming Operation," PaymentsSource website. July 11. Available online at: *www.paymentssource.com/news/becu-card-skimming-operation-busted-3006922-1.html.*

Smart Card Alliance. 2011. "Card Payment Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?" White Paper. February.

Sullivan, Richard. 2009. "The Benefits of Collecting and Reporting Payment Fraud Statistics for the United States," *Payment System Research Briefing*, Federal Reserve Bank of Kansas City. October.

_____. 2012. "The Federal Reserve's Reduced Role in Retail Payments: Implications for Efficiency and Risk." Federal Reserve Bank of Kansas City *Economic Review*, Third Quarter.

UK Cards Association. 2012a. "2011 Fraud Losses Continue Downward Trend," Press Release. March 7.

_____. 2012b. "Card Expenditure Statistics." January 24.

Wicks, Mark. 2009. "National Data Security Breach Hits Home." *Charles City Press.* February 6. Available online at: *www.charlescitypress.com/news/x955247367/National-data-security-breach-hits-home.*